

Performing private database queries in a real-world environment using a quantum protocol

Philip Chan,¹ Itzel Lucio-Martinez,² Xiaofan Mo,^{2,3} Christoph Simon,² and Wolfgang Tittel²

¹*Institute for Quantum Science and Technology, and Department of Electrical & Computer Engineering, University of Calgary, Canada*

²*Institute for Quantum Science and Technology, and Department of Physics & Astronomy, University of Calgary, Canada*

³*Beijing Institute of Aerospace Control Devices, Quantum Engineering Center, China Aerospace Science and Technology Corporation, Beijing 100854.*

We present a practical quantum protocol that allows a user to retrieve information from a database while protecting the privacy of the user (i.e. limiting the database's knowledge of what information is retrieved) as well as the privacy of the database (i.e. limiting the amount of information the user can retrieve). This functionality is similar to the cryptographic primitive 1-out-of- N oblivious transfer, which has been well studied in the context of classical information theory. While it has been shown that quantum protocols cannot provide perfect privacy against an arbitrarily powerful quantum computer, they are not vulnerable to improvements in classical computing technology or algorithms. Here we show an experimental demonstration of our new protocol over a deployed fiber channel, and present an analysis showing that our protocol is secure against simple quantum attacks. This makes private queries the second application of quantum communication (after quantum key distribution) that has been demonstrated in a real-world environment, meeting both the requirements of loss- and fault-tolerance.

Uncertainty in quantum mechanics can be used to provide security in cryptographic applications, allowing quantum cryptographic protocols to relax the typical assumptions required for security (e.g. an adversary with limited computational power), or even avoid them altogether. The use of quantum information has proven extremely successful for key distribution, where quantum key distribution (QKD) [1–3] can allow two parties to communicate over a public channel with information theoretic security (i.e. security against an adversary with arbitrarily powerful computational capability, including quantum computers). On the other hand, the security of commonly-used public-key distribution protocols [4–6], which use only classical information, relies on the complexity of certain mathematical problems. The application of quantum information theory to other cryptographic tasks is an interesting topic both because of the insight offered into capabilities of quantum versus classical information coding, and because of the possibility of developing new practical cryptographic protocols with improved security. Indeed, there are various proposals and experimental demonstrations of quantum cryptographic primitives such as secret sharing [7, 8], coin-flipping [1, 9–16], bit commitment [17, 18], and oblivious transfer (OT) [18–22]. However, of these protocols, only the bit commitment and OT protocols of ref. [17, 18] are simultaneously loss- and noise-tolerant, and thus are candidates for real-world implementation.

This article focuses on the problem of private queries, which refers to a class of protocols that either implement 1-out-of- N OT, or implement functionality similar to 1-out-of- N OT (the difference in functionality depends on the specific protocol). 1-out-of- N oblivious transfer allows a user, Ursula, to retrieve a single element from

an N -element database without the database provider, Dave, learning which element was retrieved. (Note that while Ursula and Dave wish to cooperate in order to successfully perform this query, they are also adversaries in that they can attempt to learn information that the other party wishes to keep secret.) This functionality can be useful if the database spends significant effort gathering and analyzing data (e.g. to make recommendations to investors) and the user wishes to purchase information privately from Dave [21]. (Note that, e.g. Dave knowing about interest from a large investor could affect his recommendations to other clients and/or influence the stock price.) Furthermore, interest in this topic also stems from the fact that OT has been shown to be a building block for other cryptographic primitives, such as secure two-party computation [23]. As such, OT has been well studied in classical information theory [24–26].

As with QKD, quantum protocols allow OT to be secure under less stringent assumptions than their classical counterparts. In particular it allows security against arbitrarily powerful classical computers. However, unlike QKD, it has been shown that information theoretic security against an arbitrarily powerful quantum adversary is impossible for a quantum OT protocol. In ref. [27], it was shown that, assuming a universal quantum computer, the requirements for ideal OT, (a) that Ursula is able to retrieve exactly one element, and (b) that Dave cannot gain any information about which element was retrieved, imply that Ursula can then access every element of the database. However, this does not mean that a practical protocol cannot exist. In practice, it may not be necessary to have ideal OT — that is conditions (a) and/or (b) may be relaxed, which could then lead to security against a universal quantum computer. Furthermore, reasonable

assumptions about the computational capabilities of the dishonest party may be acceptable. Indeed, classical OT protocols also rely on one of two assumptions — that at least some fraction of the intermediaries used to perform the query are trustworthy [25, 26], or that the adversary has limited classical computational resources [24]. It remains an interesting question as to whether a non-ideal quantum OT protocol can offer a practical level of privacy, and under what assumptions about Ursula and Dave’s technological capabilities a given level of privacy can be achieved.

Several quantum protocols for private queries have been proposed recently that explore the possibilities offered by making use of quantum information. Ref. [19] proposed a private query protocol that does not satisfy condition (b) above, since it allowed a dishonest Dave to gain complete information about which element Ursula retrieved. However, the protocol still offers security for Ursula as she has, in principle, the potential to detect Dave’s attempt to gain information about her query, thus discouraging Dave from cheating (this type of security is referred to as cheat sensitivity). Note that condition (a) was also not satisfied, as a dishonest user could sacrifice her ability to verify Dave’s honesty in order to obtain a second element (although, this is not a significant loss of privacy for the database if N is large). An experimental proof-of-principle demonstration of this protocol was subsequently performed [20], however, as Dave could hide his attempts to cheat if there was significant transmission loss and/or errors in the quantum channel, the protocol is not practical under realistic conditions. Ref. [21] proposed a probabilistic n -out-of- N OT protocol based on the SARG04 Quantum Key Distribution (QKD) protocol [28]. This protocol allows Dave to gain information about Ursula’s query, but only at the risk of introducing errors into the element Ursula retrieved, thereby allowing a dishonest database to be detected (hence, the protocol is cheat sensitive). The protocol also did not satisfy condition (a) above as Ursula gains probabilistic information about elements of the database she does not request. Interesting features of this protocol are the ability to tolerate loss in the channel, as well as the fact that it is simple to implement using existing QKD technology. However, noisy channels were left as an open question, preventing implementation of the protocol in realistic scenarios. The protocol we propose in this work is based on the protocol of ref. [21] and its generalization [22], and retains the advantages of those works while additionally addressing the remaining obstacle for a real-world implementation by including an error correction procedure. Interestingly, the error correction procedure also provides additional opportunities for Ursula to verify Dave’s honesty, thus enhancing the cheat sensitive property of the protocol.

Let us note that König, Wehner, and Wullschleger [18] proposed a quantum protocol for 1-out-of-2 OT using a noisy storage model, where perfect security is achieved

under the assumption that the dishonest party has imperfect quantum devices (i.e. quantum memories) which introduce increasing amounts of noise into the stored quantum states over time (this assumption is one way to preclude the universal quantum computer required by the proof [27] that ideal OT was not possible). An experimental demonstration of this work has also recently been performed [29].

RESULTS

A loss- and fault-tolerant private query protocol

As in ref. [21, 22], the goal of our protocol is to facilitate a private query on an N -bit database using an N -bit oblivious key (for simplicity, we consider each element of the database to be a single bit). The oblivious key is a string of random bits known in its entirety to Dave, but not to Ursula. To achieve ideal 1-out-of- N OT, Ursula must know a single bit of the oblivious key, whose position is unknown to Dave. Here we implement probabilistic n -out-of- N OT. In this case, Ursula will, on average, know the value of \bar{n} bits (where \bar{n} is small) with high confidence (for brevity, we often simply describe such bits as being known to Ursula). She will also have probabilistic knowledge of other bits of the oblivious key (i.e. she can guess their value with better than 50% probability). The locations of the bits Ursula knows are distributed in random positions throughout the key which are unknown to Dave. At the end of the protocol, Ursula’s probabilistic knowledge of the oblivious key is mapped to her knowledge of the database, thus the protocol does not satisfy condition (a) of ideal OT. Condition (b) of ideal OT is also not satisfied, as we retain the property that Dave can gain information about Ursula’s query at the cost of introducing errors [21, 22]. A list of possibly pessimistic assumptions under which the protocol is secure is given in the Supplementary Information. The honest protocol for the private query is as follows (see Figure 1 for a graphical representation of the protocol):

1. Dave generates two long strings of classical bits uniformly at random, and records their values. Each string should be $\approx \frac{kN}{t}$ bits in length, where k is a parameter determined by the previously agreed upon error correction procedure (to be discussed later), N is the length of the database, and t is the transmission of the link between Ursula and Dave.
2. Dave uses each pair of classical bits generated above to choose a quantum state from a set of four previously agreed upon non-orthogonal states (shown in Figure 1; note that these are not the standard BB84 states), and prepares qubits accordingly. A random bit from the first string determines whether

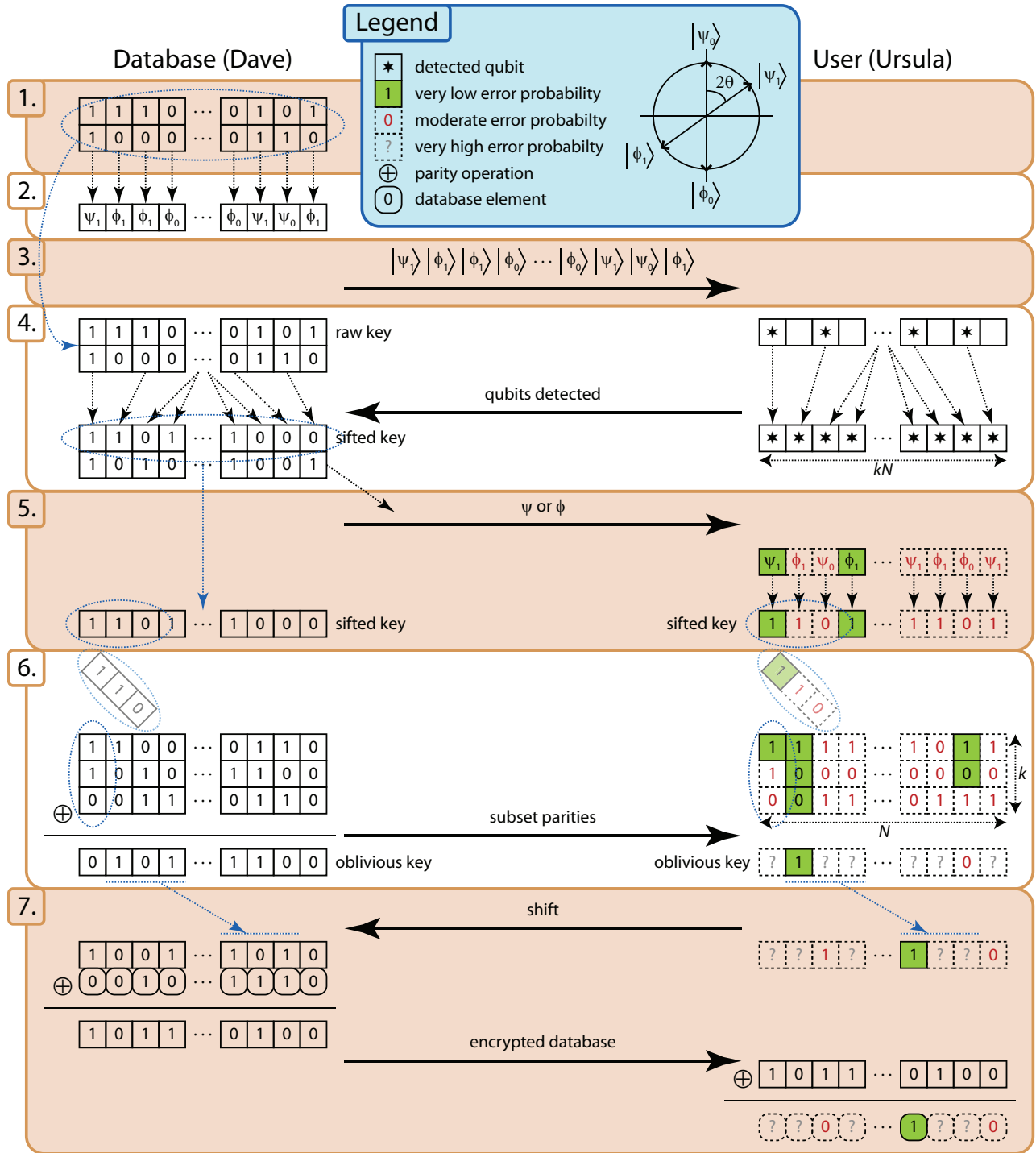


FIG. 1. Graphical representation of the private query protocol. The steps indicated on the left margin correspond to the steps described in the text.

the state is prepared in the 0-basis (spanned by $|\psi_0\rangle$ and $|\phi_0\rangle$) or the 1-basis (spanned by $|\psi_1\rangle$ and $|\phi_1\rangle$), and the corresponding random bit in the second string determines whether the ψ or ϕ state in each basis is chosen. The first random string forms Dave's raw key, for which the bit values correspond

to the bases in which he prepared the qubits.

3. Dave sends the qubits encoded into single photons to Ursula using a possibly lossy and noisy quantum channel.

4. Ursula makes projection measurements using either

the 0- or 1-basis, chosen uniformly at random, and records the measurement bases and the results. Ursula publicly announces the cases in which she detected a photon, and Ursula and Dave both discard all the events where Ursula failed to detect the photon. Note that the ability for Ursula to select bits to discard does not allow her to gain any advantage as she does not have any information from Dave at this point of the protocol. The protocol proceeds to the next step once Ursula has succeeded in detecting kN photons, and the corresponding kN bits that Dave keeps from his raw key form his sifted key.

5. Dave publicly announces his second string of random bits (used to select whether he encoded the qubits into a ψ or ϕ state), which, combined with knowledge from Ursula's measurements (and, for the moment, assuming a noiseless channel), allows her to conclusively identify whether the state was encoded in the 0- or 1-basis with probability $p_c = \frac{\sin^2(\theta)}{2}$. Note that when Ursula's measurements yielded inconclusive results, which occurs with probability $p_i = 1 - p_c$, she gains probabilistic information about the basis. This information can be quantified by the probability that she incorrectly identifies the basis, $e_i = \frac{\cos^2(\theta)}{1 + \cos^2(\theta)}$. A noisy channel will affect the probabilities p_c , p_i , and e_i , as well as result in a non-zero error rate for conclusive measurements, denoted e_c . Like Dave, Ursula associates classical bit values to the quantum states based on the basis, and forms her sifted key using the most likely values of the bits given her measurement results. Note that Ursula can abort the protocol if her results indicate that Dave's choice of quantum states deviates significantly from uniform.
6. Dave divides his sifted key into N k -bit blocks, and computes each bit of his oblivious key as the parity of the k bits in each block (the parity is 0 if an even number of the k bits is 1, and 1 otherwise). He publicly announces which bits form each block. In addition, according to a previously agreed upon error-correcting code, he also sends the parities of several subsets of the k bits to Ursula. Using this information, along with her sifted key and knowledge of whether the measurements were conclusive or inconclusive, Ursula computes the most likely value of each oblivious key bit, as well as the probability that this value is incorrect, denoted e_k . The error-correcting code is selected such that Ursula will only have a high confidence (or low e_k) in \bar{n} bits on average, where \bar{n} is typically a few bits. Note that the probabilistic nature of the protocol implies that Ursula may not learn any bits of the oblivious key, in which case the protocol must be restarted.

Selecting \bar{n} to be a few bits ensures that the probability for Ursula to not know any bits is very low, and allows Dave to abort the protocol after a small number of declared failures by Ursula. This prevents her from repeatedly declaring failure until she obtains a very favorable result (i.e. many known bits) before proceeding with the protocol [21]. Furthermore, as discussed in detail in the Supplementary Information, the errors introduced by a dishonest Dave may cause him to send classical information for error correction that is inconsistent with Ursula's measurements, in which case Ursula aborts the protocol. Note that at this point, Ursula has not revealed any information other than announcing which photons were detected.

7. Ursula selects a shift value that aligns one of the bits she knows in the oblivious key to the bit in the database that she wants to know. She communicates this shift value classically to Dave, who applies the shift to his oblivious key, and then uses it to encrypt the database using the one-time-pad [30]. He then sends the encrypted database to Ursula, who can only decrypt the bits for which she knows the corresponding oblivious key bit. If Ursula knows multiple bits of the oblivious key she will learn multiple bits of the database. However, the shift only allows her to select the location of a single bit of the database, with the remaining learned bits distributed randomly.

Error-correcting codes for private queries

Our error correction procedure (see Supplementary Information for a full description) is inspired by syndrome decoding of error-correcting codes such as Hamming codes [31], which can operate on a few bits at a time. However, it is important to note that the context of private queries creates unique requirements. First, as mentioned above, the goal of our error correction algorithm is to recover the value of the k -bit parity, and not the individual values of the k bits as would typically be the case for error correction. Second, the goal in designing the error-correcting code is not to simply maximize the probability of successful decoding (i.e. obtaining a sufficiently low value of e_k). Rather, a specific success probability is desired in order to ensure that Ursula only learns a few bits of the oblivious key. Furthermore, to prevent Ursula from learning a large amount of probabilistic information about the remaining bits of the key, it is desirable to keep e_k as high as possible in those cases where decoding does not succeed. Third, the input bits can be divided into those with low error rate (conclusive measurements), and those with very high error rate (inconclusive measurements). We note that it is the

interaction of this latter property with the short block lengths used that allows uncertainty to be maintained after error correction, thereby limiting the amount of information that Ursula learns about the database. These unique requirements make it necessary to construct error-correcting codes specifically for private queries, rather than using those designed for classical communications or QKD.

In order to quickly evaluate error-correcting codes, we define two thresholds, t_U and t_D . When $e_k \leq t_U$, Ursula considers the oblivious key bit to be known. When $e_k \leq t_D$, Dave considers Ursula to have significant partial information about that bit. These thresholds should be selected based on the requirements of the application. In this work, we use $t_U = 10^{-3}$ and $t_D = \frac{1}{3}$. In order to reduce the probability of error in Ursula's oblivious key bit below her threshold (i.e. $e_k \leq t_U$), the error correction process must sufficiently reduce e_k when her quantum measurements succeeded in obtaining a large amount of information about the k bits (e.g. when most or all measurements were conclusive). However, the error correction will also reduce e_k in the cases where several measurements were inconclusive. Hence, the error rate for inconclusive measurements, e_i , is of particular importance to the fraction of bits where $e_k \leq t_D$. With this in mind, a smaller angle between states (characterized by θ as shown in Figure 1) has, in addition to those benefits noted in ref. [22] (i.e. reduced quantum communication, improved database security, and better control over the number of bits Ursula learns), the benefit of reducing the partial information from inconclusive measurements. However, there is a trade-off between these benefits and the fact that the error rate for conclusive measurements is also increased due to a reduced signal-to-noise ratio, making it more difficult to achieve $e_k \leq t_U$. A detailed description of the selection of our error-correcting codes is given in the Supplementary Information.

Experimental and simulated performance of our protocol

We performed an experimental demonstration of private queries over a 12.4 km fiber link between the University of Calgary and SAIT Polytechnic, using our BB84 [1] QKD system [32] (with a small modification to the hardware to set $\theta = 35.6^\circ \pm 0.49^\circ$ — all other differences between our protocol and BB84 QKD are in the classical post-processing). Our experimental setup is shown in Figure 2 (see ref. [32] for a detailed description). Note that our demonstration uses weak coherent pulses rather than single photons, and hence database privacy requires the assumption that Ursula is not able to exploit pulses containing multiple photons (adapting the protocol for weak coherent pulses, e.g. using decoy states as in QKD [33–35], remains an open question, and we discuss

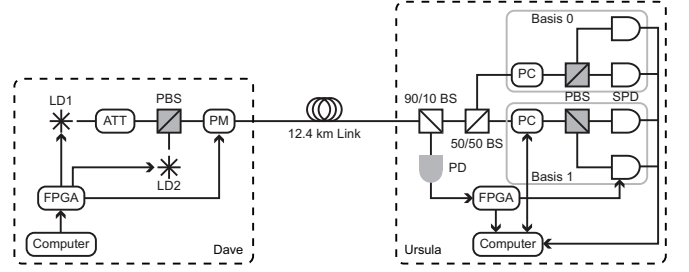


FIG. 2. Diagram of the experimental setup. The database (Dave) uses a computer and field-programmable gate-array (FPGA) to control the generation of polarization qubits via an attenuated laser diode (LD1 and ATT) and polarization modular (PM). Quantum frames [32] (sequences of strong light for timing and stabilization) are generated by a second laser diode (LD2) and merged using a polarizing beam-splitter (PBS). Light is transmitted from Dave to Ursula through a 12.4 km dark fiber link with 4.5 dB loss between SAIT Polytechnic and the University of Calgary. Ursula splits off 10% of the incoming light (90/10 BS) to a photodiode (PD) used to detect the quantum frames. The 50/50 BS is used to passively select a random measurement basis. The apparatus for each basis consists of a polarization controller (PC), a PBS, and two single photon detectors (SPD) to make the projection measurement. Upon detecting a quantum frame, Ursula's FPGA triggers the SPDs and initiates data collection by the computer, or polarization compensation, as appropriate.

some possibilities in the Supplementary Information). We consider a database size of $N = 10^6$ and, based on measured error rates for our system, an error-correcting code with $k = 10$ was selected, thus requiring 10^7 measured qubits per query. Note that we did not consider $k > 10$ due to computational constraints when searching for the best possible construction of the error-correcting code. A total of 11 queries was performed using a mean number of photons per pulse of $\mu = 0.95 \pm 0.047$ to show that the protocol can function at the single photon level. In this setting, our system took approximately 4.5 hours to accumulate the 10^7 bits of data needed for one private query. In order to quickly collect statistics, we repeated the experiment with mean number of photons per pulse increased to $\mu = 9.5 \pm 0.47$, performing 104 queries. While the multi-photon emissions at this μ are likely to compromise the security of the protocol if Ursula monitors the pulses outside Dave's laboratory, fair data collection is ensured by the fact that this value corresponds to ~ 0.95 photons per pulse at the detectors. The measured parameters that determine the performance of the protocol are shown in Table I (note that the experimentally measured parameters at both mean photon numbers are the same to within one standard deviation), along with parameters for a theoretical simulation of what could be achieved using state-of-the-art detectors [36, 37]. These detectors allow for significantly reduced noise as they feature low dark count rates (≈ 100 Hz), and, in the case of ref. [36], detection efficiencies up to 93%. With the

improved signal-to-noise ratio, we select the parameters of the protocol to be $\theta = 25^\circ$ and $k = 9$.

TABLE I. Parameters for the private query protocol as measured in our experiment with standard detectors, and simulated for low-noise detectors. The value of θ (including standard deviation) is measured using classical light. For the probabilities of conclusive measurements, p_c , and error rates for conclusive and inconclusive measurements, e_c and e_i , the standard error expected based on Poissonian counting statistics for the 10^7 bits in each query is negligible compared to the observed variations across the queries performed. The observed standard deviations are attributed to time-varying error in the alignment of the measurement bases at the receiver as a result of channel instability. Note that the measurement results for the $\mu = 9.5 \pm 0.47$ case show more variation in the parameters than for the $\mu = 0.95 \pm 0.047$ case due to short-term fluctuations that are averaged out by the long data collection time needed to acquire the 10^7 bits per query in the $\mu = 0.95 \pm 0.47$ case.

	standard detectors		low-noise detectors
μ (photons)	0.95 ± 0.047	9.5 ± 0.47	1
θ ($^\circ$)	35.6 ± 0.49	35.6 ± 0.49	25
p_c (%)	16.1 ± 0.29	16.1 ± 0.93	9.22
e_c (%)	4.4 ± 0.59	4.6 ± 0.38	1.91
e_i (%)	41.24 ± 0.08	41.3 ± 0.64	45.12
k (bits)	10	10	9

The experimental and simulated results for these codes are shown in Table II. The simulated results corresponding to our experiment are derived from Monte Carlo simulations taking into account the variation in the parameters shown in Table I. Figure 3 compares the distribution of the results over the 104 queries performed in the $\mu = 9.5 \pm 0.47$ case with the simulation results, showing good agreement between the two. Note that in both experimental cases, no errors were observed in the bits learned by Ursula (i.e. where $e_k \leq 10^{-3}$), with a total of 45 bits learned in 11 queries when $\mu = 0.95 \pm 0.047$ and 405 bits learned in 104 queries when $\mu = 9.5 \pm 0.47$.

In addition, our simulation results show that the primary obstacle to improving database security in the protocol is noise in the system, which can be greatly reduced by state-of-the-art single photon detectors. These detectors can also improve the rate at which queries can be performed by almost an order of magnitude because of their higher detection efficiencies. Further improvement of this rate is straightforward, as QKD systems can easily be adapted to perform this protocol. A state-of-the-art BB84 QKD system has shown that data can be accumulated at a rate of 10^6 to 10^7 bits per second, depending on the distance between Ursula and Dave [38]. For the parameters in our experimental demonstration, this would allow one private query to be performed every few seconds. The amount of data required can also be reduced by repeating a short oblivious key over a longer database and then applying a shift as before to allow Ursula to select the desired bit. This would allow queries to be

performed more often, or equivalently, allow queries to be performed on a larger database in the same amount of time. However, this comes at the expense of database security, as the user is able to learn additional bits for each repetition of the key (though not in locations of her choice, as only a single shift value is communicated). We also note that a modification to the protocol of ref. [21] has recently been proposed that reduces the amount of quantum communication required [39], however applying this modification to our protocol is not straightforward.

Cheating strategies

It is important to consider potential cheating strategies in view of error correction (a more detailed discussion can be found in the Supplementary Information). We considered the attacks on individual qubits discussed in ref. [21, 22], and found that they are made less powerful by error correction. First, for a dishonest database, it was shown that Dave can send false quantum states in order to manipulate Ursula's probabilities for conclusive and inconclusive measurements, p_c and p_i , giving him knowledge of Ursula's query at the expense of introducing errors [21]. With error correction, this attack only succeeds if the error correction is successful despite the additional errors introduced. Furthermore, Ursula can abort the protocol if, in the process of error correction, she detects an abnormal error rate (i.e. one that is inconsistent with the agreed upon error correcting code and success probability of the protocol) that was caused by the attack. Second, for a dishonest user, it was shown that Ursula could perform an unambiguous state discrimination (USD) measurement [40, 41] in order to slightly improve her probability of conclusive measurements, which allows her to learn a few additional bits of the oblivious key [21]. However, this comes at the expense of gaining no information about the bit value (i.e. $e_i = 0.5$) when the USD measurement gives inconclusive results. While this probabilistic information was not previously considered useful [21, 22], it is an important input to the error correction process. Thus, the effectiveness of this attack is reduced in the presence of error correction, and our analysis in the Supplementary Information shows that in some cases performing a USD measurement actually reduces the number of bits of the oblivious key that Ursula learns as compared to the honest measurements. Note that only individual USD measurements have been considered, and collective attacks (e.g. an optimized joint USD measurement on the k qubits that form each oblivious key bit) remain an open question.

In addition to the previously studied attacks, we also consider that Ursula and Dave are adversarial in nature in the protocol, and thus may not cooperate when estimating the error rate in order to select an appropriate error-correcting code. An error-correcting code that is

TABLE II. Experimental and simulated results for the quantum private queries. The following figures of merit are used: the average number of bits learned by the user per query, \bar{n} , the average proportion of the database where the user has significant partial information (i.e. $e_k \leq t_D$), \bar{m} , and the failure probability (i.e. that the user learns zero bits), P_0 .

	$\mu = 0.95 \pm 0.047$		$\mu = 9.5 \pm 0.47$		low-noise
	experimental	simulated	experimental	simulated	simulated
\bar{n} (bits)	4.1 ± 2.4	3.2 ± 1.1	3.9 ± 3.1	3.5 ± 1.9	4.35
\bar{m} (%)	6.1 ± 0.25	6.1 ± 0.25	6.3 ± 1.4	6.3 ± 1.3	0.96
P_0 (%)	9.1 ± 9.1	8.8	8.7 ± 2.9	9.4	1.29

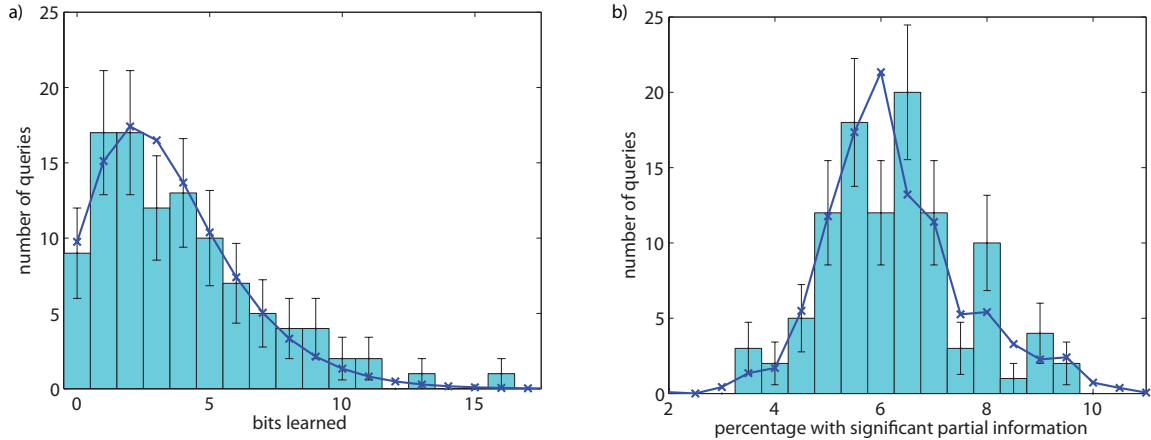


FIG. 3. Histograms for the information gained by the user in the 104 queries performed in the $\mu = 9.5 \pm 0.47$ case. a) The number of bits learned by the user. b) The percentage of the database of which the user learns significant partial information. In both figures error bars for the experimental results represent one standard deviation assuming Poissonian counting statistics, and the blue crosses show the expected distribution obtained from Monte Carlo simulations.

not well suited to the actual error rate in the system will either result in Ursula learning too few or too many bits of the oblivious key, but does not impact user security. Hence the database does not have any motivation to falsify the error rate, but the user would like the database to think the error rate is larger than it is in reality, leading to the selection of an error-correcting code that gives her more information. In our analysis (detailed in the Supplementary Information), we find that Dave can ensure that he has a reasonable level of security by determining the error rate of devices under his control (potentially by intentionally introducing noise) and selecting an error-correcting code accordingly. In addition, even if Ursula's devices introduce some additional error that Dave does not account for in his security analysis, the protocol is still successful for her.

Note that the ability to adjust the number of bits Ursula learns about the oblivious key through the selection of an appropriate error-correcting code is a useful feature for the future development of the protocol. As the security of the protocol against arbitrary quantum attacks remains an open question, it is conceivable that Ursula can make measurements which give her more information about the quantum states sent by Dave than has been considered in this work. However, if such measurements are simple to implement, they can be adopted as

the procedure for a honest user provided that the error-correcting code can be adjusted to account for the improved information gain.

DISCUSSION

We have shown that error correction can be integrated into the private query protocol proposed in ref. [21] and generalized in ref. [22], which has allowed us to perform, for the first time, a quantum protocol for private queries in a real-world setting. We have re-examined the individual attacks discussed in ref. [21, 22], and found that error correction presents additional complications for these cheating strategies. Error rate estimation between adversarial parties is not an issue in this protocol since database security can be guaranteed by the errors introduced by Dave's devices, and the user is able to tolerate additional error in the system. Quantum protocols for private queries have thus been shown to be possible in practice, and present an interesting alternative compared to non-quantum OT schemes.

ACKNOWLEDGEMENTS

The authors thank M. Jakobi, M.V. Panduranga Rao and C. Erven for useful discussions, V. Kiselyov for tech-

nical support, SAIT Polytechnic for providing laboratory space, and acknowledge funding by NSERC, Quantum-Works, General Dynamics Canada, iCORE (now part of AITF), AITF, CFI, and AAET.

SUPPLEMENTARY INFORMATION

QUANTUM STATE IDENTIFICATION

In our protocol, the database provider, Dave, encodes each qubit into one of four randomly chosen quantum states, $|\psi_0\rangle$, $|\psi_1\rangle$, $|\phi_0\rangle$ or $|\phi_1\rangle$, as shown in Figure 4. The user, Ursula, measures each qubit in either the 0-basis, spanned by $|\psi_0\rangle$ and $|\phi_0\rangle$, or the 1-basis, spanned by $|\psi_1\rangle$ and $|\phi_1\rangle$. After these measurements, Dave tells Ursula whether each qubit was encoded into one of the ψ states or one of the ϕ states. In order to demonstrate the state identification process, suppose Ursula measured in the 0-basis, and Dave declares that he sent one of the ψ states. If Ursula's measurement result was $|\phi_0\rangle$, she knows Dave could not have sent $|\psi_0\rangle$ as these two states are orthogonal. Hence Dave must have sent $|\psi_1\rangle$. This is a conclusive result, and occurs with probability $p_c = \frac{\sin^2(\theta)}{2}$. Alternatively, if Ursula's measurement result was $|\psi_0\rangle$, she only knows that the state was more likely to have been $|\psi_0\rangle$ than $|\psi_1\rangle$. This is an inconclusive result, occurring with probability $p_i = 1 - p_c$. As the two potential states are associated with different classical bit values (as indicated by the subscripts), Ursula only gains probabilistic knowledge from this measurement result. This corresponds to an error rate of $e_i = \frac{\cos^2(\theta)}{1+\cos^2(\theta)}$ in the ideal case (i.e. when no other sources of error are present).

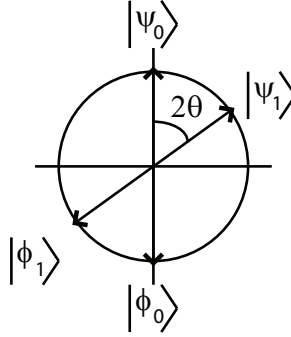


FIG. 4. Quantum states used in the private query protocol shown on a plane of the Bloch sphere.

ERROR CORRECTION

We use a parity-based forward error-correcting code operating on k -bit blocks (corresponding to the k bits used to compute one oblivious key bit), where Dave sends the parity of several subsets of the k bits to Ursula. The construction of the code is normally described as a parity check matrix, denoted \mathbf{H} , and is known to both Ursula and Dave. The parity computation for the j^{th} oblivious key bit is then given by:

$$\vec{p}_j = \mathbf{H}\vec{d}_j \pmod{2} \quad (1)$$

where \vec{p}_j is a vector of computed parity bits (which Dave sends to Ursula) and \vec{d}_j is a vector containing the k bits that Dave uses to compute a single oblivious key bit. For each oblivious key bit, Ursula has a corresponding k -bit vector, \vec{u}_j , where each bit stems from a conclusive or an inconclusive measurement that have, respectively, error rates of e_c and e_i . Ursula can estimate these error rates over the entire protocol by comparing the parities, \vec{p}_j , she receives from Dave and the parities she computes locally using \vec{u}_j . Using these error rates, Ursula's error correction procedure for each oblivious key bit is as follows:

1. Rule out those combinations of values for the k bits that are not consistent with the values for \vec{p}_j received from Dave.
2. Divide the remaining possibilities into two sets — those that correspond to an oblivious key bit of 0, and of 1.
3. Based on the measurement results and estimated error rates, calculate the probability that each combination of values for the k bits is correct. The set with the higher total probability determines the most likely value of the oblivious key bit.
4. Compute the probability of error in the oblivious key bit, e_k .

Note that Ursula can significantly reduce the computation required for error correction by only performing this procedure when almost all of the k bits were measured conclusively. In doing so, she only performs error correction when there is a possibility that the result will satisfy $e_k \leq t_U$.

The error correcting codes used in this work are given by:

$$\mathbf{H}_{35.6} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (2)$$

for $\theta = 35.6^\circ$ and

$$\mathbf{H}_{25} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} \quad (3)$$

for $\theta = 25^\circ$.

ASSUMPTIONS REQUIRED FOR SECURITY

The results for honest parties presented in the main text and for the cheating strategies discussed the following section rely on several assumptions. These assumptions are that:

1. Quantum theory is correct and complete.
2. Ursula's and Dave's laboratories are secure (i.e. no information leaves their laboratories except for as specified in the protocol).
3. The dishonest party has limited quantum technological capabilities. At the fundamental level, some amount of security is guaranteed by the no-signaling theorem (protecting the user's security) and the impossibility to perfectly distinguish between non-orthogonal quantum states (protecting the database's security) [21]. The experimental results presented in Table 2 and Figure 3 of the main text are valid assuming an arbitrarily powerful classical computer, and in the following section we discuss simulations showing the effect of several quantum attacks on those results (as well as the technological requirements for those attacks). It remains an open question as to what specific technological assumptions, if any, are required to achieve a sufficient level of security. In addition, we note that the error-correcting code in our protocol can be selected in order to provide less information to Ursula in order to compensate for an increased information gain from more powerful quantum measurements. Thus, it may be possible to adopt such measurements as the legitimate procedure for the user, provided that the measurements are feasible technologically.
4. In our experimental demonstration, it is also necessary to assume that the user is not able to take advantage of multi-photon pulses that result from using a source of weak coherent pulses. While this assumption can be avoided if Dave uses a single photon source, the implementation of weak coherent pulses is much simpler from

a technological perspective. Thus, it is desirable for the protocol to be secure for weak coherent pulses without the need for additional assumptions. The decoy state techniques used in QKD [33–35] provide security against an adversary capable of exploiting multi-photon pulses. However, the adversarial nature of the parties in private queries means these techniques cannot be applied directly as they require cooperation between the legitimate parties. Adapting these protocols for private queries is an interesting open question. Another possibility for security with weak coherent pulses is for Dave to account for the additional information that can be extracted from multi-photon pulses, which is well studied in the context of QKD, when selecting the error-correcting code. If this information gain due to multi-photon pulses is sufficiently small, the protocol can provide a suitable level of database security while maintaining a high success probability for the user.

CHEATING STRATEGIES

In this section we discuss the attacks on individual qubits proposed in [21, 22]. The discussion below shows that the error correction step provides improved security for the protocol against these individual attacks. Optimization of collective attacks in view of error correction remains an interesting open question, as does an analysis of fully general quantum attacks or an information theoretic treatment of our protocol. Furthermore, we comment on the issue of error rate estimation between adversarial parties. As example cases for these discussions, we consider the mean parameters measured with $\mu = 0.95 \pm 0.47$ using standard detectors and the simulated parameters for low-noise detectors (see Table 1 in the main text). For the measured parameters, we do not consider the observed variances since they are specific to the system used to implement the honest protocol.

User Privacy

Let us first consider an attempt by the database to determine which piece of information Ursula is interested in. Recall that our protocol does not prevent a dishonest database from gaining some information about Ursula’s query, but is cheat sensitive in that it gives Ursula the possibility of detecting such an attack. Performing the attack described below does not require any additional technology, as it simply requires Dave to send quantum states that either maximize or minimize the probability, p_c , that Ursula will believe her measurement was conclusive [21]. In order to determine Ursula’s query, Dave seeks to have Ursula learn only a single bit of the oblivious key whose position is known to him, thus he maximizes p_c for the k bits that form one oblivious key bit in an attempt to convince Ursula that she knows a particular bit of the oblivious key of his choice. He then minimizes p_c elsewhere in an attempt to prevent Ursula from knowing other bits in the oblivious key, in positions unknown to him. As noted in [22], Dave’s ability to control p_c improves as the angle between the 0-basis and 1-basis, θ , is decreased, making the attack more powerful. However, in both cases (i.e. maximization or minimization of p_c), the quantum state Dave sends for this attack lies directly between either pair of ψ or ϕ states shown in Figure 4, and thus Ursula will associate a bit value to the measurement that is completely unknown to Dave. Hence, under this attack, Ursula receives a random bit value in response to her query, leading to the cheat sensitive property in [21, 22] (and in our protocol), where incorrect query results will reveal Dave’s dishonest behavior (i.e. over time, Dave will acquire a reputation of providing poor query results).

Furthermore, in our protocol the error correction steps provide additional opportunities for Ursula to verify Dave’s honesty, both weakening the above attack as well as providing the possibility of detecting the weakened attack prior to Ursula revealing information about her query. Specifically, the consequence of Dave sending quantum states that minimize p_c (in order to prevent Ursula from knowing one or more bits of the oblivious key in random positions) is that Ursula’s and Dave’s sifted keys are completely uncorrelated (i.e. they have error rates $e_c = e_i = 50\%$). Additionally, since Dave has no knowledge of Ursula’s sifted key, the parity bits, \vec{p}_j (see Eq. 1), that he sends for error correction will be completely uncorrelated with the parity bits Ursula computes from her measurement results. This allows Ursula to detect a cheating database, and abort the protocol. While this severely restricts Dave’s ability to ensure that Ursula does not know bits of the oblivious key in random positions, it does not prevent him from attempting to convince Ursula that she knows a bit in a particular position of his choosing in addition to any bits she learns randomly (in this case, Dave is unsure if Ursula’s query corresponds to the position where he conducted the attack, or to an unknown position that Ursula learned randomly). This is due to the fact that Dave only needs to maximize p_c in k bits out of kN bits of the sifted key, which has a negligible effect on the overall error rates for large N . However, this attack has a limited success probability, and if it fails, it may fail in a way that is suspicious to Ursula, again

allowing Ursula to abort the protocol (see below for a detailed example). Note that the above verifications occur after the error correction step, but before the shift value is communicated, thus Dave gains no information about Ursula’s query if the protocol is aborted.

To illustrate the possibility for Ursula to detect an attempt by Dave to convince her a particular bit is known, we consider the parameters as discussed above. For $k = 10$ and $\theta = 35.6^\circ$, there is a 37.49% chance that Ursula will believe all k bits are conclusive given this attack. For $k = 9$ and $\theta = 25^\circ$, this probability increases to 64.93%. However, for Dave to convince Ursula that she knows a particular bit of the oblivious key, it is not sufficient for her to believe that all k bits are conclusive, as the error correction procedure must also indicate that her measurement results are correct or correctable (i.e. the error correction procedure results in a error probability $e_k \leq t_U$, where we recall that we have selected $t_U = 10^{-3}$ as the threshold where Ursula considers a bit to be known). The attack thus becomes more difficult with error correction, since the database must also send parity information to Ursula that is consistent with her measurements. Since Dave’s bit values are completely uncorrelated with Ursula’s measured bit values, the parity information that Dave sends is essentially random, and Ursula is unlikely to find a low value for e_k . In the above examples, Ursula finds $e_k \leq 10^{-3}$ with only 5.92% probability and 12.73% probability, respectively, showing that this attack has a limited success probability. In addition, the case where Ursula believes all k bits were measured conclusively is of particular interest as it is very unlikely that she will find a large probability of error in the oblivious key bit after error correction, e_k , if the protocol was performed honestly. However, in the above attack, Dave must send parity information that is uncorrelated with Ursula’s measurement results, leading to a large amount of uncertainty during Ursula’s error correction process and resulting in a high probability of finding a large value for e_k . For example, when Ursula believes all k bits were measured conclusively, for $k = 10$ and $\theta = 35.6^\circ$, she expects $e_k \geq 0.15$ with 2.14% probability if Dave is honest, but this increases to 40.63% given the above attack. For $k = 9$ and $\theta = 25^\circ$, she expects $e_k \geq 0.055$ with 0.71% probability when honest, and 65.63% with the attack. A large value for e_k when all k bits are measured conclusively can thus serve as an indication that Dave is attempting to cheat, and allow Ursula to abort the protocol. Furthermore, even if the protocol proceeds and Dave is cheating (e.g. because Dave, by chance, sent consistent parity information), Ursula’s and Dave’s oblivious key bits after error correction are still uncorrelated, as in the protocol of [21, 22]. This ensures that the cheat sensitive property of the protocols in [21, 22] discussed above is preserved in our protocol.

Generally speaking, we note that the additional benefits provided by the error correction procedure are relevant to other attack strategies as well. Ursula now has the ability to monitor the aggregate error rates in the system, allowing her to detect any attack by Dave that has a significant effect on the overall error rates. Furthermore, the need for the database to be able to send meaningful parity information during error correction provides an additional hurdle for attacks that cause Dave to lose information about Ursula’s measurement results.

Database Privacy

On the other hand, a user attacking the protocol seeks to learn as many bits from the database as possible. One method of doing so is to store the photons from Dave in a quantum memory until after he reveals whether he sent a ψ or ϕ state, and then perform an unambiguous state discrimination (USD) measurement [40, 41] to distinguish which of the two remaining states was sent. However, as Dave only reveals information about a quantum state after Ursula has declared that a photon has been detected, every photon that a dishonest Ursula declares as “detected” contributes to her sifted key. As such, any photon that Ursula declares as “detected” but subsequently fails to detect (e.g. because she could not identify when a photon was successfully stored in her quantum memory, or because of losses occurring after the declaration) results in bits in the sifted key of which Ursula has no knowledge. Successfully performing an USD attack thus requires a heralding signal indicating that a photon was successfully stored in the quantum memory, and the ability to recall the photon from the quantum memory with near 100% efficiency. For the following analysis, we assume a heralding signal in conjunction with a perfect quantum memory (i.e. one that introduces no error into the quantum states, and has 100% efficiency; a realistic quantum memory would reduce the effectiveness of the attack), and that there are no other sources of loss that reduce the success probability of the USD measurement.

If Ursula is able to perform an USD measurement, this allows her to maximize the probability that the quantum measurements will give conclusive results. As shown in [21], the probability of conclusive results increases only slightly when performing USD measurements, resulting in the user only learning a few more bits than when making honest measurements. Furthermore, the advantage decreases as θ is decreased [22]. Additionally, in the presence of error correction, the advantage of performing an USD measurement further decreases. This is because the USD

TABLE III. Comparison of simulation results for a user experiencing higher error rates than those that Dave uses to select an error-correcting code. The columns labeled “user” correspond to experimental results obtained using standard detectors ($\theta = 35.6^\circ$, $k = 10$), or simulation results with improved detectors ($\theta = 25^\circ$, $k = 9$), as taken from Tables 1 and 2 of the main text, and represents the actual results of the protocol. The columns labeled “database” represent the potential results of the protocol, based on an error rate estimation considering only noise at the database.

	$\theta = 35.6^\circ$, $k = 10$		$\theta = 25^\circ$, $k = 9$	
	user	database	user	database
p_c (%)	16.1	15.9	9.22	9.14
e_c (%)	4.4	2.5	1.91	1.38
e_i (%)	41.24	40.89	45.12	45.11
\bar{n} (bits)	3.89	14.32	4.35	10.67
\bar{m} (%)	6.03	6.69	0.96	0.93

measurement gains no information from inconclusive results, essentially exchanging this information for an increased probability of obtaining a conclusive result. However, the partial information from inconclusive results is useful during error correction, and can even allow Ursula to know the value of the oblivious key bit in some instances in which not all measurements were conclusive. As such, error correction can hinder the effectiveness of the USD attack. Performing USD measurements when using the code with $k = 10$ and $\theta = 35.6^\circ$ only increases the average number of bits the user knows from $\bar{n} = 3.89$ to $\bar{n} = 11.15$ — a rather small gain for a database of 10^6 bits. For the code using $k = 9$ and $\theta = 25^\circ$, performing USD measurements decreases the average number of bits the user knows from $\bar{n} = 4.35$ to $\bar{n} = 1.00$. This decrease is due to the fact that at this smaller value of θ , the value of the partial information gained from inconclusive measurements outweighs the slightly improved probability for a conclusive measurement offered by the USD measurement. Note that these results are based on having the same error rate as for the honest measurements, which may not be a realistic assumption given that a different measurement apparatus is required. The issue of error rates differing from those used to select the error-correcting code is addressed separately below so as to isolate this effect from that of the USD measurement.

Error rate estimation

Finally, since Ursula and Dave have an adversarial nature in the private query protocol, accurately characterizing the error rate in the system in order to select an error-correcting code is not straightforward. In particular, Ursula would like the database to believe the error rate is higher than in reality, as Dave would then select an error-correcting code that gives her more information, allowing her to learn more bits from the database. To avoid this problem, Dave can determine the amount of information a user will learn from the protocol based solely on the error introduced by devices directly under his control. In fact, he can even choose to deliberately introduce additional noise in order to provide the desired level of database security. Additional imperfections in the system would cause the user to experience a higher error rate than Dave’s estimate, leading to her learning fewer bits than the database predicts. To show that there is a regime that allows the protocol to succeed from the user’s perspective while still providing good database security, we re-examine the error-correcting codes that we have considered thus far using the parameters shown in the columns labeled “database” in Table III, where noise in the system has been reduced compared to the original parameters in the main text (shown in the columns labeled “user”). Note that the effect of the lower noise observed by the database is not just a lower error rate in the conclusive measurements, e_c , in the “database” columns — the other parameters are affected as well. The error rates for inconclusive measurements, e_i , is affected by the same noise sources as e_c , but the effect on e_i is smaller as the error for inconclusive measurements is dominated by uncertainty inherent in the quantum measurement. Hence, e_i in the “database” columns is only slightly lower than in the “user” columns. The total number of conclusive results is reduced slightly as the number of conclusive results recorded due to noise events is lower. Hence, the probability of conclusive measurements, p_c , is lowered slightly in the “database” columns. Table III also shows the results for the average number of bits learned by the user, \bar{n} , and the average proportion of the database where Dave considers Ursula to have significant partial information, \bar{m} , for the original parameters in the “user” columns, as well as for a lower error rate that can be used to select the error-correcting code in the “database” columns. As can be seen, the reduction in error rates does not result in a large increase in the potential amount of information gained by a user who experiences no additional error. Thus, it is possible for an error-correcting code to be selected based on local error rates to both provide the database with good security and allow the protocol to be successful for a user experiencing higher error rates.

-
- [1] Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* 175–179 (1984).
 - [2] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
 - [3] Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
 - [4] Rivest, R. L., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120–126 (1978).
 - [5] Miller, V. S. Use of elliptic curves in cryptography. In *Advances in Cryptology, CRYPTO '85*, 417–426 (1986).
 - [6] Koblitz, N. Elliptic curve cryptosystems. *Mathematics of Computation* **48**, pp. 203–209.
 - [7] Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829–1834 (1999).
 - [8] Tittel, W., Zbinden, H. & Gisin, N. Experimental demonstration of quantum secret sharing. *Phys. Rev. A* **63**, 042301 (2001).
 - [9] Aharonov, D., Ta-Shma, A., Vazirani, U. V. & Yao, A. C. Quantum bit escrow. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing, STOC '00*, 705–714 (2000).
 - [10] Ambainis, A. A new protocol and lower bounds for quantum coin flipping. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing, STOC '01*, 134–142 (2001).
 - [11] Molina-Terriza, G., Vaziri, A., Ursin, R. & Zeilinger, A. Experimental quantum coin tossing. *Phys. Rev. Lett.* **94**, 040501 (2005).
 - [12] Nguyen, A. T., Frison, J., Phan Huy, K. & Massar, S. Experimental quantum tossing of a single coin. *New J. Phys.* **10**, 083037 (2008).
 - [13] Chailloux, A. & Kerenidis, I. Optimal quantum strong coin flipping. In *Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on*, 527–533 (2009).
 - [14] Berlín, G., Brassard, G., Bussi eres, F. & Godbout, N. Fair loss-tolerant quantum coin flipping. *Phys. Rev. A* **80**, 062321 (2009).
 - [15] Aharon, N., Massar, S. & Silman, J. Family of loss-tolerant quantum coin-flipping protocols. *Phys. Rev. A* **82**, 052307 (2010).
 - [16] Berl n, G. *et al.* Experimental loss tolerant quantum coin flipping. *Nat. Commun.* **2**, 561 (2011).
 - [17] Ng, N. H. Y., Joshi, S. K., Ming, C. C., Kurtsiefer, C. & Wehner, S. Experimental implementation of bit commitment in the noisy-storage model. *Nat. Commun.* **3**, 1326 (2012).
 - [18] K nig, R., Wehner, S. & Wullschlegel, J. Unconditional security from noisy quantum storage. *Information Theory, IEEE Transactions on* **58**, 1962–1984 (2012).
 - [19] Giovannetti, V., Lloyd, S. & Maccone, L. Quantum private queries. *Phys. Rev. Lett.* **100**, 230502 (2008).
 - [20] De Martini, F. *et al.* Experimental quantum private queries with linear optics. *Phys. Rev. A* **80**, 010302 (2009).
 - [21] Jakobi, M. *et al.* Practical private database queries based on a quantum-key-distribution protocol. *Phys. Rev. A* **83**, 022301 (2011).
 - [22] Gao, F., Liu, B., Wen, Q.-Y. & Chen, H. Flexible quantum private queries based on quantum key distribution. *Opt. Express* **20**, 17411–17420 (2012).
 - [23] Kilian, J. Founding cryptography on oblivious transfer. In *Proceedings of the twentieth annual ACM symposium on Theory of computing, STOC '88*, 20–31 (1988).
 - [24] Rabin, M. O. How to exchange secrets by oblivious transfer. Tech. Rep., Harvard University (1981).
 - [25] Naor, M. & Pinkas, B. Distributed oblivious transfer. In *Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT '00*, 205–219 (2000).
 - [26] Blundo, C., D'Arco, P., De Santis, A. & Stinson, D. On unconditionally secure distributed oblivious transfer. *Journal of Cryptology* **20**, 323–373.
 - [27] Lo, H.-K. Insecurity of quantum secure computations. *Phys. Rev. A* **56**, 1154–1162 (1997).
 - [28] Scarani, V., Ac n, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92**, 057901 (2004).
 - [29] Erven, C., Wehner, S., Gidov, N., Laflamme, R. & Weihs, G. An experimental implementation of oblivious transfer in the noisy storage model. *manuscript in preparation* (2013).
 - [30] Vernam, G. S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *American Institute of Electrical Engineers, Transactions of the* **XLV**, 295–301 (1926).
 - [31] MacKay, D. *Information Theory, Inference, and Learning Algorithms* (Cambridge University Press, 2003).
 - [32] Lucio-Martinez, I., Chan, P., Mo, X.-F., Hosier, S. & Tittel, W. Proof-of-concept of real world quantum key distribution with quantum frames. *New J. Phys.* **11**, 095001 (2009).
 - [33] Hwang, W.-Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
 - [34] Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
 - [35] Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
 - [36] Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nat. Photon.* **7**, 210–214 (2013).
 - [37] Yan, Z. *et al.* An ultra low noise telecom wavelength free running single photon detector using negative feedback avalanche diode. *Review of Scientific Instruments* **83**, 073105–073105–15 (2012).

- [38] Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. J. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Opt. Express* **16**, 18790–18979 (2008).
- [39] Panduranga Rao, M. V. & Jakobi, M. Towards communication-efficient quantum oblivious key distribution. *Phys. Rev. A* **87**, 012331 (2013).
- [40] Herzog, U. & Bergou, J. A. Optimum unambiguous discrimination of two mixed quantum states. *Phys. Rev. A* **71**, 050301 (2005).
- [41] Raynal, P. Unambiguous state discrimination of two density matrices in quantum information theory. *arXiv:quant-ph/0611133v1* (2006).